Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for communicating to a server machine a certificate of a user sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is an HTTP or an equivalent protocol, and a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and the security module, said method comprising:

inserting said certificate into a cookie header of a request in the first protocol, and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine.

2. (Previously Presented) A method according to claim 1, further comprising:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header.

3. (Previously Presented) A method according to claim 1, further comprising:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine, and

creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (Currently Amended) A method according to claim 3, further comprising:

adding a specific cookie into the existing or new cookie header, and assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

5. (Previously Presented) A method according to claim 1, further comprising:

transmitting to the server machine the request sent by the client machine into which the certificate has been inserted.

6. (Previously Presented) A security machine for securing exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is an HTTP or an equivalent protocol, and a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and said security machine, said security machine comprising:

an analyzer for enabling the transmission of a certificate into a cookie header of an HTTP or equivalent request.

7. (Previously Presented) A system comprising:

a client machine,

a server machine, and

a security module,

wherein a first protocol used between the client machine and the server machine is an HTTP or an equivalent protocol, wherein a second security protocol such as SSL or an equivalent protocol is implemented between the client machine and the security module, and wherein the security module comprises an analyzing program for enabling transmission of a certificate sent by the client machine into a cookie header of an HTTP or equivalent request.

8. (Previously Presented) A program integrated into a security module that allows the method according to claim 1 to be executed when the program is run in a machine.